UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/554,275	10/25/2005	Andreas Lindinger	2004P12244WOUS	2989

29177   7590   04/06/2009

K&L Gates LLP
P.O. BOX 1135
CHICAGO, IL 60690

EXAMINER
NGUYEN, TRONG H

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
04/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 February 2009</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-5</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-5</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is in response to the communication filed on 02/05/2009. In response

to the office action mailed on 09/10/2008, claims **1-5** have been amended. Pending

claims include claims **1-5**.

The objection to the title of the invention has been withdrawn due to applicants'

amendment.

The objection to the drawings has been withdrawn due to applicants'

amendments.

The objection to claim **5** has been withdrawn due to applicants' amendment.

Response to Arguments

2.   Applicants' arguments filed 02/05/2009 have been fully considered but the

following arguments are not persuasive.

a) Applicants argued that:

i. Rune fails to teach or suggest "comparing <u>by the first </u>subscriber the fetched

identifier with the identifiers stored in the memory", as expressly recited in

independent claim 1.

ii. Rune also fails to teach or suggest "if a matching identifier is present,

prompting the security certificate associated with the identifier to be a basis for a

subsequent data transmission", as expressly recited in independent claim 1.

iii. Rune is concerned only with encrypting radio traffic between a terminal and a general access <u>network</u> (GAN), and neither teaches nor suggests providing secure communication between a tachograph and a memory card located in a vehicle, or that such an encrypted communication network would or could be used with small scale devices, such as a tachograph and memory card.

iv. Hsu is concerned only with providing an improved wireless point to multipoint communication system (see paragraph [0004] of Hsu). The list of Hsu is maintained by an <u>access point</u> for all the subscriber units in the access point's center. The list disclosed by Hsu has nothing to do with a tachograph memory storing driver card identifiers.

b) In response to applicants' arguments:

i. As seen on page 6, lines 4-7 of prior office action, Rune discloses **"comparing** <u>**by the first subscriber**</u> **the fetched identifier with the identifiers stored in the memory"** as [The terminal initiates contact by registering with a specific GAN (but not necessarily setting up a call). A processor in the terminal compares the received GAN identifier with the stored identifiers" (Col. 5, lines 42-45)]. *Note that the terminal stores* **at least** *one public key and a GAN identification character that identifies* **a specific GAN associated with that key** *(Rune, Col. 5,*

*lines 36-42). Therefore, the terminal communicates with **at least** one GAN. As a result, the terminal is analogous to the first subscriber.*

ii. Rune discloses "**if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for a subsequent data transmission**" as ["and if a match can be made (and the key has not expired), the processor retrieves the stored public key associated with the identified GAN" (Col. 5, lines 44-47) and "the same public key can be used for all subsequent communications with that GAN" (Col. 6, lines 54-55). By teaching using the retrieved public key in subsequent communications, Rune also teaches using the associated security certificate in subsequent data transmissions such as to verify the authenticity of the public key and/or its owner. *Note that Rune discloses when a public key is to be transferred from a GAN to a terminal, the key can be transferred with a public key "certificate". This certificate provides proof that the associated public key and the owner of that key are authentic. A "trusted" third party can issue the public key along with the certificate, which includes a "digital signature" that authenticates the third party's identity and the public key. The certificate can also contain the GAN's identity and the expiration date of the certificate, if any (Col. 10, lines 43-51). Thus, since the certificate associated with a public key provides proof that the associated public key and the owner of that key are authentic, it is important to prompt the associated certificate and*

check its expiration date to make sure it has not been expired each time a public

key is about to be used to detect any invalid public key].

iii. Rune's invention relates to secure data communications and even though it is disclosed as being used between a communications terminal and a mobile communications network as an exemplary embodiment, Rune's method can be used to secure communication between other devices.   There is no specific mentioning in Rune that this method of secure communications can not be used in securing communications between small scale devices such as a tachograph and a memory card.   In fact, Rune specifically mentions that "Although a preferred embodiment of the method and apparatus of the present invention has been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, **it will be understood that the invention is not limited to the embodiments disclosed**, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims" (Col. 11, lines 31-38) (emphasis added). Moreover, on page 1, lines 12-16 of the instant specification, applicants also recognize that "methods for secure data transmission are becoming increasingly important and already exist in many diverse forms in the field of computer networks.   Comparable in the wider sense with modern computer networks is also the interaction or the secure data transmission of a digital tachograph and a memory card on the basis of EC regulation 3821/85".

iv. Hsu's method of maintaining a dynamic MAC-SU list (shown in Fig. 6) with each entry containing a MAC address of a user device associated with the subscriber unit, the subscriber identification number, and a timestamp corresponding to the time at which the entry was created or updated and deleting the oldest entry with the new entry when the list is full allows an access point to effectively monitor which user devices are currently active, save memory space and effectively support a much greater number of user devices (Col. 4, Par. 0056). Rune's invention also involves maintaining a list of GAN's identifiers (and associated certificates) at a communication terminal and reducing radio transmission delays, saving network transmission time and increasing data throughput (Col. 6, lines 11-14). Thus, it is obvious to a person of ordinary skill in the art at the time of the invention to improve Rune's invention using Hsu's method for the purpose of allowing a terminal to effectively monitor which GANs are currently active, save memory space and effectively support a greater number of GAN.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims **1-3** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune

US 5,850,444 (hereinafter "Rune"), in view of European Digital Tachograph Common

Security Guide (hereinafter "CSG"), and further in view of Hsu et al. US 2004/0063438

(hereinafter "Hsu").

Regarding claim **1**, Rune discloses "**A method for secure data transmission**

between a first subscriber and second subscribers" and "**having at least one**

respective data store" as ["a method and apparatus for encrypting radio traffic

between terminals and a mobile communications network" (Col. 1, lines 8-10)] "**wherein**

the first subscriber has a memory which stores a particular number of entries,

each comprising identifiers and associated certificates from the second

subscribers, the method comprising the steps of:" as ["The terminal stores at least

one public key in the non-volatile memory. Along with each public key, the terminal also

stores a respective expiration date for the key, and a GAN identification character that

identifies a specific GAN associated with that key" (Col. 5, lines 36-40). Furthermore,

Rune discloses "when a public key is to be transferred from a GAN to a terminal, the

key can be transferred with a public key 'certificate' (Col. 10, lines 43-45). It is obvious

to the terminal if desired to store certificates associated with public keys for use in

subsequent transmissions as Rune mentioned "This certificate provides proof that the

associated public key and the owner of that key are authentic" (Col. 10, lines 45-47)]

"**fetching an identifier by the first subscriber from a connected second subscriber**

of the second subscribers, the connected second subscriber being connected to

the first subscriber;" and "**comparing by the first subscriber the fetched identifier with the identifiers stored in the memory;**" as ["The terminal initiates contact by registering with a specific GAN (but not necessarily setting up a call). A processor in the terminal compares the received GAN identifier with the stored identifiers" (Col. 5, lines 42-45). *Note that the terminal stores **at least** one public key and a GAN identification character that identifies **a specific GAN associated with that key** (Rune, Col. 5, lines 36-42). Therefore, the terminal communicates with **at least** one GAN. As a result, the terminal is analogous to the first subscriber*] "**if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for subsequent data transmission**" as ["and if a match can be made (and the key has not expired), the processor retrieves the stored public key associated with the identified GAN" (Col. 5, lines 44-47) and "the same public key can be used for all subsequent communications with that GAN" (Col. 6, lines 54-55). By teaching using the retrieved public key in subsequent communications, Rune also teaches using the associated security certificate in subsequent data transmissions such as to verify the authenticity of the public key and/or its owner. *Note that Rune discloses when a public key is to be transferred from a GAN to a terminal, the key can be transferred with a public key "certificate". This certificate provides proof that the associated public key and the owner of that key are authentic. A "trusted" third party can issue the public key along with the certificate, which includes a "digital signature" that authenticates the third party's identity and the public key. The certificate can also contain the GAN's identity and the expiration date of the certificate, if any (Col. 10, lines 43-51). Thus, since the*

certificate associated with a public key provides proof that the associated public key and

the owner of that key are authentic, it is important to prompt the associated certificate

and check its expiration date to make sure it has not been expired each time a public

key is about to be used to detect any invalid public key] **"if no matching identifier is**

stored in the memory, prompting the first subscriber to perform security

certificate verification with the connected second subscriber" as ["However, in the

event that no such match is found, the terminal sends a request for the GAN to transmit

a public key" (Col. 5, lines 47-49). In addition, Rune discloses "a problem can arise if an

unauthorized user attempts to impersonate a GAN and transmit a public key to the

terminal. In that event, as described below, the terminal can be configured to

authenticate the received public key and the identity of the GAN. For example, when a

public key is to be transferred from a GAN to a terminal, the key can be transferred with

a public key 'certificate'." (Col. 10, lines 38-45). By teaching authenticating the received

public key and the identity of the GAN, Rune also teaches verifying the associated

certificate accompanying that public key.]

Rune does not specifically disclose **"first subscriber being a tachograph in a**

commercial vehicle and the second subscribers being memory cards", **"with a**

detection time for the security certificate", **"updating the detection time for the**

security certificate to a current system time", and **"in the event of verification,**

storing an entry corresponding to the verified security certificate with a current

detection time in the memory with the entry with the oldest detection date being

replaced by the new entry if a particular number of entries has already been reached".

CSG discloses common security guideline for a digital tachograph system for motor vehicles comprising tachograph cards and recording equipment (vehicle unit and motion sensors) wherein each tachograph card has a card ID, secret and public keys and public keys certificate and each vehicle unit has a vehicle identification (VU ID), secret and public keys, and public keys certificates (Pages 10, 20-21 and 23).

CSG and Rune are analogous art because they are in the same field of endeavor of secure data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to adopt Rune's method of secure data transmission to be used in data communications between other devices such as in communication between a tachograph and memory card by having the tachograph storing identifiers and associated certificates, fetching an identifier from the memory card, comparing this identifier with stored identifiers, and performing certificate verification with the memory card if no match is found for the purpose of ensuring that personal information remains confidential during communications between the recording equipment and tachograph cards (CSG, Page 12, lines 8-9; Page 14, lines 17-20).

Hsu discloses "a MAC-SU list manager 69" which "has multiple entries 102" and the "entry also includes a time stamp 108 corresponding to the time at which the entry was created or updated" (Par. 0051, lines 14-16). Furthermore, Hsu discloses "When the MAC-SU list is full, and the microprocessor needs to install an additional entry, the

microprocessor scans the index group to which the new entry applies, finds and deletes

the oldest entry (i.e. the entry with the earliest time stamp) in the group, and enters the

new entry" (Par. 0056, lines 7-12).

Hsu, Rune, and CSG are analogous art because they are in the same field of

endeavor of data communication.

It would have been obvious to a person of ordinary skill in the art at the time of

the invention to enhance the method of data transmission between the tachograph and

memory card of Rune in view of CSG by including a time stamp or detection time for

each certificate, updating the detection time to current system time when the certificate

is used, and in the process of certificate verification storing an entry corresponding to

the verified certificate by replacing the entry with the oldest detection time with the new

entry with the current detection time if the particular number of entries has been

reached in order to save memory space and "in this manner, the system constantly

updates the MAC-SU List to include those user devices that are currently active" (Hsu,

Par. 0056, lines 15-17).

Regarding claim **2**, Rune discloses "**wherein the identifier is a public key from

an RSA method from the connected second subscriber**" as ["a mobile terminal

stores at least one public key, along with a unique identification character of at least one

GAN associated with that public key, in memory location" (Col. 4, lines 16-19) and "the

GAN can maintain one or more asymmetric public key/private key pairs. In that event, a

so-called 'RSA Algorithm' can be used to create the public key/private key pairs" (Col. 7,

lines 1-2). By teaching a unique identification character associated with a public key

and using the RSA algorithm to create the public key/private key pairs, Rune also

teaches that the unique identifier can be a RSA public key from the second subscriber.]

Regarding claim **3**, Rune discloses "**wherein a subsequent data transmission

is effected in TDES-encrypted form, with verification of the security certificates

being followed by both subscribers sending a random number in encrypted form

to the other subscriber and both subscribers independently of one another each

using the two random numbers to determine a common key for data transmission

using the same algorithm**" as ["a so-called Diffie-Hellman 'exponential key exchange'

algorithm can be used to let the terminal and the GAN agree on a secret session key"

(Col. 9, lines 50-53), "The terminal (118) generates the random number X_T ($1<X_T<q-1$),

and computes the value $Y_T=a^{X}_T$ mod q. The GAN (e.g., the RNC or base station)

generates the random number X_G ($1<X_G<q-1$), and computes the value of $Y_G=a^{X}_G$ mod

q (Col. 9, line 66-Col.10, line 3), "Y_T and Y_G are transferred unencrypted to the

respective GAN and terminal" (Col. 10, lines 6-7). Then, both the terminal and the GAN

independently generates the "communications session encryption key" K_S (Col. 10, line

13-14). Furthermore, Rune discloses "A known symmetric encryption algorithm can be

used to encrypt and decrypt the ensuing radio traffic with the secret key, such as, for

example, a one, two or three pass Data Encryption Standard (DES) algorithm" (Col. 9,

lines 44-47). Though, Rune discloses Y_T and Y_G are transferred unencrypted to the

respective GAN and terminal, it is obvious that Y_T and Y_G can be transferred encrypted

if one is desired to do so.]

5.   Claims **4-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune

in view of CSG, and further in view of Hsu, and further in view of Kostal et al. US

7,308,573 (hereinafter "Kostal").

Regarding claim **4**, Rune in view of CSG and further in view of Hsu discloses

"The method according to claim 1 wherein the verification of the certificate from

the first subscriber by the connected second subscriber and vice versa" but does

not specially disclose "**and vice versa**" and "**comprises the following n number of**

steps: in the first step, the connected second subscriber sends the first

subscriber a first security certificate which the connected second subscriber

subject to verification using a first public key and in doing so ascertains a second

public key, and if the verification results in authenticity then the first step is

repeated (n-1) times using a further transmitted security certificate and the

second public key ascertained in the previous step instead of the first public key,

with a new second public key and a verification result always being obtained."

However, Kostal discloses "The process of validating the digital signatures in a

chain" (Col. 15, lines 37-38) wherein "knowledge of the public key corresponding to the

private key of the trusted authority is gained, and such public key of the trusted authority

is employed to verify the signature of the root certificate in the chain. Presuming the

root certificate signature verifies, then, the public key from the root certificate is obtained

and employed to verify the signature of the first intermediate certificate in the chain.

The process repeats serially through the chain until every signature thereof is verified"

(Col. 16, line 65-Col. 17, line7). By teaching a method of verifying a chain of certificate

above, Kostal also teaches a method of verifying multiple certificates from a single subscriber with multiple public/private key pairs and in the process ascertaining the subscriber's public keys.   Furthermore, Kostal also teaches that this certificate verification process comprises n number of steps if the user has n number of certificates.

Kostal, Rune, CSG, and Hsu are analogous art because they are in the same field of endeavor of data transmission and security.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to enhance the method of data transmission between the tachograph and memory card of Rune in view of CSG, and further in view of Hsu by having both subscribers mutually verify each other's certificates by first verifying all certificates of one subscriber using the method as disclosed by Kostal above and then verify the other subscriber's certificates also using the same method in order to authenticate both subscribers and hence resulting in a stronger security level between the two subscribers.

Regarding claim **5**, by disclosing the process of verifying multiple certificates in n number of steps by Kostal, barring any unexpected result, it would have been obvious that the number of steps can be 3 which is one instance of n.

Conclusion

6.   Examiner cites particular columns and line numbers in the references as applied to the claims for the convenience of the applicant. Although the specified citations are

representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

7.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Ernst-G. Giessmann, Specification Version 1.0 of the Security Target TCOS Tachograph Card, 05/07/2004, T-Systems International GmbH, Version 1.0, Pages 46-48, 56-63.

8.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/T N/
Examiner